EXHIBIT 27

This is an archived version of the Chrome privacy notice. View the current privacy notice.

Google Chrome Privacy Notice

Archive date: September 1, 2015

Chromecast is covered by the Google Privacy Policy. Learn more.

The Google Privacy Policy describes how we treat personal information when you use Google's products and services, including when you use Chrome browser and Chrome OS to access those products and services.

This Google Chrome Privacy Notice describes the privacy practices that are specific to the Chrome family of products. This includes the Chrome browser, Chrome OS, and Safe Browsing. Some of the features described in this Privacy Notice are available in other web browsers (e.g. you may choose to use Safe Browsing features in Mozilla Firefox), so remember that you should also read the privacy policy for the browser in which the features are running.

Not all of the features discussed in this Privacy Notice appear in all Chrome products. To keep things simple, however, we're going to use the term "Chrome" on its own to refer to each of the products within the Chrome family. Where an individual Chrome product works in a different way we'll be sure to highlight that.

For early adopters who want to test features that are still under development, we make available preview versions (also known as beta, dev and canary) of Chrome browser and Chrome OS in addition to the stable version. Although this Google Chrome Privacy Notice applies to the stable and preview versions, it may not be fully up to date when describing features still under development in the preview versions.

Google will notify you of any material changes to this policy, and you will always have the option to use Chrome in a way that does not send any personally identifiable information to Google, or to remove your information and discontinue using it.

For step-by-step guides to help manage your privacy preferences read our guide to Browsers, Google Chrome, Privacy and You.

Information Google receives when you use Chrome

You do not need to provide any personally identifying information in order to use Chrome.

When you use any browser, including Chrome, to contact Google's servers, by default Google receives standard log information including your system's IP address and one or more cookies. You can configure Chrome browser and Chrome OS to not accept cookies from Google or other sites. Learn more about configuring cookies and site data in Chrome browser and Chrome OS.

If you use Chrome to access other Google services, such as using the search engine on the Google homepage or checking Gmail, the fact that you are using Chrome does not cause Google to receive any special or additional personally identifying information about you.

In addition, some Chrome features may send limited additional information to Google or your default search engine:

- If you use the Multiple Users feature of Chrome browser, you can set up personalized copies of Chrome browser for users who are sharing the same computing device. It isn't intended to secure your data against other people using your device - so anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system.

- If you choose Google as your search engine, Chrome will contact Google when it starts or when you change networks so as to determine the best local web address to send search queries. When you type URLs or queries in the Chrome address bar (omnibox) or App Launcher search box, the letters you type may be sent to your default search engine so that the search engine's prediction feature can automatically recommend terms or URLs you may be looking for. Additionally, for signed in users, the text that you type into the App Launcher search box can be sent to Google to provide recommendations for the contacts and the apps you might be looking for. If you accept a predicted query or URL, Chrome may send that information from the browser to your default search engine as well. Learn more about disabling server predictions in the omnibox and Google's logging policies for omnibox predictions.

- On mobile versions of the Chrome browser, you can enable "Touch to Search" which allows you to tap on a word to see a suggested search term. The word you tapped, the content of the page, and the URL of the page you're on will be sent to Google to provide the recommended search term.

- If you enable the feature in your device's Today view, you can use Chrome on your iPhone or iPad to discover objects around you that are broadcasting web addresses as part of the Physical Web. When you use this feature, Chrome sends the web addresses broadcast by these objects to a Google server to find the title of the web page and help rank the results. The information sent to Google to provide this feature does not include any personal information from your device.

- If you navigate to a URL that does not exist, Chrome may send the URL to Google so we can help you find the URL you were looking for. We may also use this information in an aggregated way to help other web users - e.g. to let them know that the site may be down. Learn more about disabling suggestions on navigation errors.

- Chrome periodically contacts Google to perform functions such as checking for updates, checking connectivity status, validating current time, and estimating the number of active users. Each copy of Chrome browser includes a temporary randomly-generated installation number which will be sent to Google when you install and first use the product. The temporary number will be promptly deleted the first time that Chrome browser automatically checks for updates. If you received or reactivated your copy of the Chrome browser as part of a promotional campaign, it may also generate a non-unique promotional tag which is sent to Google when performing searches with Google and a unique token which is sent to Google when you first run and use the browser after installation, reinstallation, or reactivation. Chrome OS may send a non-unique promotional tag to Google periodically (including during initial set up) and when performing searches with Google. Furthermore, field trials may result in different variations of Chrome, and Chrome may send non-unique information to Google about which variation is active.

- If you grant an application, extension, or website permission to use Google's Cloud Messaging, or if you use Chrome Sync, Chrome generates a randomly chosen device ID. This device ID is shared with Google but not accessible to third parties, and is revoked once it is no longer in use or when the Chrome profile is removed. From the device ID, Chrome then derives a registration ID that is shared with applications, extensions, or websites to securely pass messages from Google's servers to the browser.

- Chrome OS contacts Google during initial device setup to determine if the device is subject to

policies of an enterprise administrator. This process involves sending Google a part of a hash of a short-lived device identifier and receiving back from Google a list of hashed device identifiers that were possible matches, so Chrome OS may determine if the device is on that list.

- Chrome contacts Google for session policies when a user first signs in to Chrome or starts browsing without signing in (excluding Guest mode) on devices subject to policies. Chrome will check periodically for updates to policies. Enterprise policies may involve status and activity reporting for Chrome (including location information for Chrome OS devices) set up by the enterprise admin.

- If you sign in to Chrome browser, Chrome OS or an Android device that includes Chrome as a preinstalled application with your Google Account, this will enable the synchronization feature. Google will store certain information, such as history, bookmarked URLs as well as an image and a sample of text from the bookmarked page, passwords and other settings, on Google's servers in association with your Google Account. Information stored with your Account is protected by the Google Privacy Policy. We also store this information to make it available to you on other instances of Chrome in which you choose to sign in. Learn more about the specific information you may select to synchronize, and more about disabling Chrome's synchronization feature in Chrome browser.

- If you are signed into Chrome with your Google Account, Google Drive and Docs, Sheets, Slides and Drawings will be automatically enabled for offline use. In that case, or if you otherwise enable offline use of a Google application in Chrome browser or install a Chrome application that stores data in your Google Drive account, Chrome may contact Google's servers and synchronize your data with a local copy to enable offline functionality.

- If you create a supervised user in Chrome browser or on Chrome OS with your Google Account, Google will synchronize and store certain information, such as the supervised user's history and other settings on Google's servers in association with your Google Account. We store this information in order to make it available to you at chrome.com/manage. Information stored with your account is protected by the Google Privacy Policy.

- If you use the Translate feature of Chrome, it will send the text you choose to be translated to Google for translation.

- If you use the Spellcheck feature of Chrome, which lets you use the same technology used in

Google search to check your spelling, it will send the text you type to Google for spelling and grammar suggestions.

- If you use the speech input feature of Chrome, it will send Google an audio recording of your spoken query, your default browser language and the grammar settings of the web page for which you are using speech input. Google will use this information to convert the recorded audio into text. If you have enabled usage statistics and crash reports and you use the speech input feature, additional information will be sent to Google, including the URL of the website using speech input, your operating system, and the manufacturer and model of the computing device and audio hardware you are using.

- If you use Chrome's AutoFill feature, which automatically completes web forms for you based on similar forms you have filled out before, Chrome will send Google limited information about the pages that have web forms, including a hashed URL of the web page and details of the form's structure, so that we can improve our AutoFill service for this web form. While the information that Chrome sends may include the fact that you typed information into the form, the actual text that you type in the fields will not be sent to Google unless you choose to store that data in your Google Account using Chrome's synchronization feature.

- Some web forms handled by Chrome will offer you the option to use Google Payments rather than Chrome's AutoFill feature to complete the form and make payments. If you use Google Payments, then to protect you from fraud, Chrome will collect information about your computer (including its location) and share it with Google Payments.

- If you use Chrome's location feature, which allows you to share your location with a web site, Chrome will send local network information to Google Location Services to get an estimated location. Learn more about Google Location Services and enabling / disabling location features within Google Chrome. The local network information may include (depending on the capabilities of your device) information about the wifi routers closest to you, cell IDs of the cell towers closest to you, the strength of your wifi or cell signal, and the IP address that is currently assigned to your device. We use the information to process the location request and to operate, support, and improve the overall quality of Chrome and Google Location Services. The collected information described above will be anonymized and aggregated before being used by Google to develop new features or products and services, or to improve the overall quality of any of Google's other products and services.

- If you are using a mobile version of Chrome, and you have granted your Android device or Chrome on iOS permission to access your location, then Chrome may use your location for Google location-enabled services, including for example enhancing omnibox searches.

- If you attempt to connect to a Google website using a secure connection, and the browser blocks the connection due to information that indicates you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google for the purpose of helping to determine the extent of the attack and how the attack functions.

- If you enable Chrome's "Reduce data usage" feature on your mobile device, Chrome will send your HTTP traffic through Google's optimizing servers to reduce the amount of data downloaded and improve performance. The optimizing service is disabled for connections to HTTPS origins, and for connections made from Incognito tabs.

- For Chrome browser and Chrome OS, you may choose to send usage statistics and crash reports to Google. You can manage this setting within the Chrome preferences page; for Chrome OS users, usage statistics and crash reports are enabled by default. This setting will apply to all users for a given installation of Chrome. The usage statistics and crash reports help us diagnose problems, help us understand how users interact with Chrome, and help us improve Chrome's performance.

- Chrome tries to avoid sending information that identifies you personally. Crash reports, however, can contain system information at the time of a malfunction, and errors leading up to a malfunction. We may share with third parties certain aggregated, non-personal information we derive from our analysis, such as how frequently certain types of crashes occur.

Information Google receives when you use the Safe Browsing feature on Chrome or other browsers

Google Chrome and certain third party browsers (including some versions of Mozilla's Firefox and Apple's Safari) includes Google's Safe Browsing feature. Safe Browsing sends and receives information between the browser you are using and Google's servers about suspicious websites -- for example when you visit a site that is suspected to be a phishing or malware site.

Your browser will contact Google's servers periodically to download the most recent "Safe Browsing" list,

containing known phishing and malware sites. Google does not collect any account information or other personally identifying information as part of this contact, but it does receive standard log information, including an IP address and one or more cookies. The most recent copy of the list is stored locally on your system.

Each site you visit will be checked against the Safe Browsing list on your system. If there is a match against the list, your browser will send Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. Read more information about how this works.

In addition, the following Safe Browsing features are specific to Chrome:

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and executable file downloads not already known by Google. Information regarding a potentially harmful site or executable file download (including the full URL of the site or executable file download) may be sent to Google to help determine whether the site or download is harmful. Google does not collect any account information or other personally identifying information as part of this contact, but does receive standard log information, including an IP address, URL visited and one or more cookies.

- Chrome uses Safe Browsing technology to scan your computer periodically to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. If such software is detected, Chrome may offer you the option to download the software removal tool to remove it.

- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware. This data is sent when you close or navigate away from a Safe Browsing warning page. The reports contain data, such as the URL and contents of the website as well as the URL of the page that directed you to that site, that can be used by Google to verify whether the site is still serving content that may exploit users.

- If usage statistics are enabled in Chrome and you visit a site that we think could be potentially harmful, certain additional data will be shared with Google, including the full URL that you visited, the "`referer`" header sent to that page, and the URL that matched the Safe Browsing list.

- You can always choose to disable the Safe Browsing feature within Chrome.

Information website operators receive when you visit a site using Chrome

Sites that you visit using Chrome will automatically receive standard log information similar to that received by Google. These sites may also set their own cookies or store site data on your system. You can restrict cookies and other site data in Chrome's preferences page.

If Chrome's network actions prediction features are enabled, Chrome may look up the IP addresses of all links on webpages and open network connections to load webpages faster. Sites can also use pre-rendering technology to pre-load the links that you might click next.

If you use Chrome in incognito mode or guest mode, it will not transmit any pre-existing cookies to sites that you visit. Sites may deposit new cookies on your system while you are in these modes; these cookies will only be temporarily stored and transmitted to sites while you remain in incognito / guest mode. They will be deleted when you close the browser, close all open incognito windows or exit guest mode.

If you choose to use Chrome's location feature, this service allows you to share your location with a site. Chrome will not allow a site to access your location without your permission. Google does not have control over third party websites or their privacy practices. Please carefully consider any website's privacy practices before consenting to share your location with that website.

Information stored on your system when you use Chrome

Chrome stores some information locally on your system. This may include:

- Basic browsing history information, for example the URLs of pages that you visit, a cache file of text and images from those pages, and a list of some IP addresses linked from pages that you visit.
- A searchable index of most pages you visit (except for secure pages with "https" web addresses, such as some bank pages)
- Thumbnail-sized screenshots of most pages you visit

- Cookies or web storage data deposited on your system by websites you visit
- Locally-stored data saved by Add-ons
- A record of downloads you have made from websites

You can always choose to delete your browsing history information, in whole or in part.

You can also limit the information Chrome stores on your system by using incognito mode or guest mode. The Chrome browser offers both modes. Incognito mode is useful if you would still like to have access to information from your existing profile, such as suggestions based on your browsing history, while you are browsing. Guest mode is useful if you would prefer to begin a browsing session without seeing information from any existing profiles. In either of these modes, Chrome will not store basic browsing history information such as URLs, cached page text, or IP addresses of pages linked from the websites you visit. It will also not store snapshots of pages that you visit or keep a record of your downloads (although this information could still be stored elsewhere on your system, e.g. in a list of recently opened files). New cookies received in these modes will not be saved after you close your browser, close all open incognito windows or exit guest mode. You can see when you are in incognito / guest mode because the incognito icon appears in the top corner of your browser; in some cases the border of your browser window may also change color.

When you make changes to your browser configuration, such as by bookmarking a web page or changing your settings, this information is also saved. These changes are not affected by incognito / guest mode.

You can choose to have Chrome save your passwords for specific websites. Stored passwords can be reviewed in Chrome settings.

Unique Identifiers for Digital Rights Management

In order to allow certain content to be accessed using Chrome browser for Windows or Chrome OS, Chrome may be required to provide selected content partners and websites using Adobe Flash Access with a unique identifier that is stored on your system. You can disable this feature in the settings or reset the unique identifier's value by reinstalling the operating system.

Parties to whom your unique identifier is provided could associate it with personally-identifiable information you provide to them. Google's use of a unique identifier to provide content from Google servers is subject to the Google Privacy Policy. If you are accessing content from a third party service, you should review those parties' privacy policies to learn more.

Using apps, extensions, themes, services, and other add-ons with Chrome

You may use apps, extensions, themes, services and other add-ons ("Add-ons") with Chrome, including some that may be pre-installed or integrated with Chrome and some that you may obtain from Chrome Web Store or other sources.

Before installing an Add-on, you should review the requested permissions. Add-ons may be designed to store, access, and share data stored locally or in your Google Drive account. Add-ons may use notifications that are sent through Google servers. Chrome may check for, download, and install updates to your Add-ons. Chrome may send usage indicators to Google for installed Add-ons. Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of such an identifier by removing the add-on from Chrome.

From time to time, Google may discover an Add-on that poses a security vulnerability or violates the developer terms for Chrome Web Store or other legal agreements, laws, regulations or policies. Chrome may periodically download a list of such Add-ons from Google's servers, and Google may remotely disable or remove such Add-ons from user systems in its sole discretion.

Add-ons developed and provided by Google may communicate with Google servers and are subject to the Google Privacy Policy unless otherwise indicated. Add-ons developed and provided by third parties are the responsibility of such third parties and may be subject to third party privacy policies. For example, a version of the Adobe Flash Player plug-in is preinstalled with Chrome. Adobe's website at www.adobe.com provides more information on Adobe's privacy practices with regard to Flash Player, and you can learn more about disabling Flash Player or any other plug-ins.

Uses

Information that Google receives when you use Chrome is processed in order to operate and improve Chrome and other Google services. Information that other website operators receive is subject to the privacy policies of those websites. Chrome stores information on your system in order to improve Chrome's performance and to provide you with useful features and services.

More information

Google adheres to the US Safe Harbor privacy principles. For more information about the Safe Harbor framework or our registration, see the Department of Commerce's web site.

Further information about Chrome is available here.

For more information about our privacy practices, go to the full privacy policy. If you have additional questions, please consult this page.